

PIX/ASA 7.x : CAC - Cisco VPN Client のスマートカードの認証

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[Cisco ASA の設定](#)

[配備上の考慮事項](#)

[認証、許可、アカウントティング \(AAA \) 設定](#)

[LDAP サーバの設定](#)

[トラストポイントの管理](#)

[キーの生成](#)

[CA トラストポイントのインストール](#)

[ルート証明書のインストール](#)

[ASA の登録と ID 証明書のインストール](#)

[VPN の設定](#)

[トンネル グループおよびグループ ポリシーの作成](#)

[トンネル グループ インターフェイスおよびイメージの設定](#)

[IKE/ISAKMP パラメータの設定](#)

[IPsec パラメータの設定](#)

[OCSP の設定](#)

[OCSP レスポンダ証明書の設定](#)

[OCSP を使用するための CA の設定](#)

[OCSP ルールの設定](#)

[Cisco VPN Client の設定](#)

[Cisco VPN Client の開始](#)

[新しい接続](#)

[リモート アクセスの開始](#)

[付録 A : LDAP マッピング](#)

[シナリオ 1 : リモート アクセス許可ダイヤルインを使用した Active Directory の強制 : アクセスの許可/拒否](#)

[Active Directory の設定](#)

[ASA の設定](#)

[シナリオ 2 : アクセスを許可または拒否するためのグループ メンバーシップを使用した Active Directory の強制](#)

[Active Directory の設定](#)

[ASA の設定](#)

[付録 B : ASA CLI 設定](#)

[付録 C : トラブルシューティング](#)

[AAA および LDAP のトラブルシューティング](#)

[例 1 : 正しい属性マッピングによる接続の許可](#)

[例 2 : 設定が誤った Cisco 属性マッピングによる接続の許可](#)

[認証局および OCSP のトラブルシューティング](#)

[IPSEC のトラブルシューティング](#)

[付録 D : MS 内の LDAP オブジェクトの確認](#)

[LDAP Viewer](#)

[Active Directory サービス インターフェイス エディタ](#)

[関連情報](#)

概要

このドキュメントでは、認証に Common Access Card (CAC) を使用してネットワークのリモート アクセスに関して Cisco 適応型セキュリティ アプライアンス (ASA) を設定する例を紹介します。

このドキュメントでは、Cisco ASA と Adaptive Security Device Manager (ASDM) 、 Cisco VPN Client、Microsoft Active Directory (AD) および Lightweight Directory Access Protocol (LDAP) の設定について扱います。

このガイドの設定では、Microsoft AD および LDAP サーバを使用します。またこのドキュメントでは、OCSP および LDAP 属性マップなどの高度な機能についても扱います。

前提条件

要件

Cisco ASA、Cisco VPN Client、Microsoft AD/LDAP、および公開キー インフラストラクチャ (PKI) について基本的な知識があれば、完全な設定を理解する上で役立ちます。AD グループ メンバーシップ、ユーザ プロパティ、および LDAP オブジェクトについて理解していれば、証明書属性と AD/LDAP オブジェクトの間での許可プロセスの関連付けに役立ちます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ソフトウェア バージョン 7.2(2) を実行する Cisco 5500 シリーズ 適応型セキュリティ アプライアンス (ASA)
- Cisco Adaptive Security Device Manager (ASDM) バージョン 5.2(1)
- Cisco VPN Client 4.x

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

Cisco ASA の設定

このセクションでは、ASDM を使用した Cisco ASA の設定について扱います。ここでは、IPSec 接続を経由した VPN リモート アクセス トンネルを配備するために必要なステップについて説明します。認証には CAC 証明書が使用され、証明書内のユーザ プリンシパル名 (UPN) 属性が、許可のために Active Directory に取り込まれます。

配備上の考慮事項

- このガイドでは、インターフェイス、DNS、NTP、ルーティング、デバイス アクセス、ASDM アクセスなどの基本的な設定については扱いません。ネットワーク オペレータはこれらの設定をよく理解しているものとします。詳細については、『[多機能型セキュリティアプライアンス](#)』を参照してください。
- いくつかのセクションは、基本的な VPN アクセスのために必要な必須の設定です。たとえば、OCSP 検査や LDAP マッピング検査なしで CAC カードを使って VPN トンネルを設定できます。DoD では OCSP チェックが規定されていますが、OCSP を設定しなくてもトンネルは機能します。
- 必須の基本 ASA/PIX イメージは 7.2(2) と ASDM 5.2(1) ですが、このガイドでは暫定ビルド 7.2.2.10 および ASDM 5.2.2.54 を使用します。
- LDAP スキーマの変更は不要です。
- ポリシーを強制するための LDAP およびダイナミック アクセス ポリシーのマッピングの例については、[付録 A](#) を参照してください。
- LDAP オブジェクトを MS でチェックする方法については、[付録 D](#) を参照してください。
- 詳細については、「[関連情報](#)」を参照してください。